DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF

STEPHEN J. MCHALE
DEPUTY ADMINISTRATOR
TRANSPORTATION SECURITY ADMINISTRATION

ON CIVIL AVIATION SECURITY

BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
November 20, 2003

Good morning Mr. Chairman, Congressman Waxman, and Members of the Committee. On behalf of Admiral Loy, I am pleased to appear before you today to discuss the advances in civil aviation security made by the Transportation Security Administration (TSA) and recent events involving the smuggling of prohibited items aboard aircraft.

TSA was established just two months after the September 11 attacks on our Nation when, on November 19, 2001, President Bush signed the Aviation and Transportation Security Act (ATSA). TSA is now a proud part of the Department of Homeland Security (DHS). With guidance and direction from the Border and Transportation Security Directorate, TSA and its sister agencies, the Bureau of Customs and Border Protection (CBP), the Bureau of Immigration and Customs Enforcement (ICE), the Bureau of Citizenship and Immigration Services (CIS), and the Federal Law Enforcement Training Center (FLETC), are working together to strengthen security at our borders and in our transportation systems.

TSA and its many partners have built an entirely new aviation security system that offers significantly higher levels of security than were in place in September 2001. We have built a system of rings of security—a system of systems that does not solely rely on any one component. We continuously gather as much information as possible about the threats, vulnerabilities, trends, and conditions of the aviation system and its environment. We use this domain awareness to prioritize and direct resources and take protective action. TSA's Transportation Security Intelligence Service receives, assesses, and distributes intelligence on threats to transportation and operates an around-the-clock intelligence watch tied to all national intelligence and law enforcement intelligence programs. It maintains direct connections with TSA's field operations and the security centers of major transportation stakeholders. Airport access controls and airport perimeter security are strengthened, and we have required background checks to be performed on more than a million air carrier and airport employees with unescorted access to airport secured and sterile areas. Highly trained, qualified personnel screen every bag and every passenger using state-of-the art metal detectors. All checked baggage is screened using a

combination of explosives detection systems (EDS), explosives trace detection machines (ETD), and where necessary, other congressionally approved methods of screening. TSA-certified canine teams perform multiple tasks throughout the entire airport environment, including screening checked baggage, searching unattended bags, searching vehicles approaching terminals during increased threat levels, screening cargo on a limited basis, and responding to bomb threats. The number of Federal Air Marshals has increased from just a handful on 9/11 to thousands today, and they are now deployed on high-risk domestic and international flights. Commercial aircraft serving the U.S. are equipped with new, hardened cockpit doors. TSA's Federal Flight Deck Officer program trains, equips, and deputizes pilots who volunteer to defend the flight decks of passenger aircraft as the last line of defense. By the end of FY04, at the current pilot application rate, we expect to have trained thousands of pilots who have volunteered for the program and met the initial background requirements.

Each of these security enhancements is an additional obstacle that a terrorist would have to overcome in order to accomplish his objective. Each has been carefully developed with attention to security, customer service, and a minimum impact on the flow of commerce.

TSA inherited a 30-year-old passenger-screening system designed to detect obvious weapons such as guns, hunting knives, and grenades, and has transformed it into a system that also finds much smaller and less obvious threats. We take pride in the professionalism and diligence shown by TSA screeners every day in their efforts to ensure the safety of the traveling public. Since February 2002, TSA has intercepted more than 1500 firearms and more than 54,000 box cutters. Nevertheless, there is no such thing as a zero failure rate for passenger screening. The individual components that comprise our rings of security are filters; they are not guarantees. Taken together, the combination of security measures compensates for the potential weaknesses of a particular component.

During the past several months, the media has reported on improvised explosive devices secreted in ordinary items that passengers might carry onto an airplane, and continued attempts by terrorists to perfect the shoe bomb apparatus employed, unsuccessfully, by convicted terrorist Richard Reid in December 2001. Our daily intelligence reports frequently contain information on new methods that terrorists might employ against the transportation security system. We also receive daily reports from airports on secreted prohibited items and other suspicious items that our screeners discover. These threats are a stark reminder that we must maintain our focus on security through reasonable and prudent, but effective measures efficiently applied. The number of prohibited items that TSA screeners continue to intercept from passengers is still large. In June, July, and August of this year, the number of weapons, explosives, and other prohibited items that our screeners intercepted increased by 28 percent over the number of prohibited items intercepted in the same time period in 2002, even though we have reduced the list of prohibited items to eliminate non-lethal items such as nail clippers. Among the items recently intercepted were a knife concealed inside a sealed soda can, a sword hidden inside a cane, and a gun secreted in a child's teddy bear.

On October 16, 2003, a maintenance technician for Southwest Airlines found two types of prohibited items, liquid bleach secreted in a suntan lotion bottle and boxcutters, as well as molding clay, matches, and an anonymous note in the rear lavatory of an aircraft in New Orleans. That night, similar items were found on another Southwest aircraft. When notified, TSA was able to initiate a record search quickly and link these situations to an email that TSA's Contact Center had received in September. The email included the sender's identity and details of his actions but did not include an overt threat. He was identified in less than 12 hours and interviewed in less than 20 hours from the time of notification to TSA. In those first 12 hours TSA also contacted the principal security officer of every U.S. air carrier and issued a directive that they perform fleet-wide security inspections within 24 hours.

Because the circumstances surrounding this incident are now the subject of a Federal investigation, it would be inappropriate for me to provide further information in this setting. Instead, I will focus on the steps that TSA has taken to prevent it from reoccurring.

First, the channel through which TSA received the email needed additional attention. TSA's Contact Center has been the focal point for receiving comments on travelers' experiences in screening and for reporting lost or damaged property, but not for receiving security alerts. The Contact Center receives an average of more than 5,000 telephone calls and e-mails each week, the vast majority reflecting the types of concerns noted above. The email that TSA received through this channel was not viewed as a threat, but clearly it should have received priority treatment as a potentially serious message involving security information and illegal activity.

TSA has swiftly changed procedures at its Contact Center and throughout TSA. Contact Center electronic mail, telephone calls, and other communications are now filtered for security content, reviewed by a security analyst, and when appropriate, transmitted to our Transportation Security Coordinating Center and other units for action. Contact Center personnel are trained each month on how to identify potential security violations, threat information, and criminal activity conveyed through telephone calls or other means. In addition, all TSA employees and contractors have been given specific protocols to follow in identifying, documenting, and reporting potential threat communications.

We know that there is more to do. Well before this recent episode, TSA was assessing its vulnerabilities and moving forward on a plan for screener improvement. TSA conducts an aggressive covert testing program that challenges screeners to detect threat objects at screening checkpoints and in checked baggage using simulated terrorist threat devices and current techniques. Between September 2002 and October 2003, our Office of Internal Affairs and Program Review (OIAPR) conducted 847 checkpoint and 2,737 airport security access tests, as well as computer assisted passenger prescreening (CAPPS) and checked baggage tests at 107 airports. We conduct covert testing at over three times the annual rate of the old FAA "red teams," and our testing uses more difficult, realistic testing situations. Although TSA cannot discuss the results of our tests in detail in this setting, results have shown an improvement of approximately 10 percent

from September 2002 to August 2003. This progress is particularly significant because the difficulty of the tests has increased over the past year.

The U.S. General Accounting Office (GAO) published a report in September 2003 of its preliminary observations on progress made in airport passenger screening, which was based in part upon its own covert tests and tests performed by the DHS Office of Inspector General (OIG), in addition to the OIAPR tests. This report notes the continuing need to improve screener performance and to implement performance measures to determine the effectiveness of screening operations. We concur with that finding.

In July of this year, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, we gathered data from multiple sources to determine the actual, current level of performance and the root causes for the gap between desired and actual performance.

Based upon the Screener Performance Improvement Study, TSA identified an array of specific follow-up actions. These enhancements are now being implemented under TSA's Short-Term Screening Improvement Plan outlined below.

1. Increased Federal Security Director (FSD)[1] Support and Accountability. Under TSA's plan, airports with below-par performance on covert tests will receive special attention. Teams of industrial engineers, trainers, performance consultants, and technology and management experts will identify the causes for poor performance at these airports and work with FSDs to design and implement solutions. Follow up will include additional covert testing and FSD accountability for any continued performance deficiency. We will also create incentive programs to encourage top performance.

2. Enhanced Training for Screeners and Supervisors. National, validated skill standards for all screeners form the foundation of an integrated system for hiring, training, certifying, and measuring performance. All screeners must demonstrate the qualifications, knowledge, skills, and aptitudes necessary to meet Federal standards and successfully perform as a transportation security screener. They receive a minimum of 40 hours of classroom instruction and 60 hours of on-the-job training. Screeners are subject to periodic proficiency assessments and unannounced performance testing. They are made aware of new threats and methods of concealment.

Screeners who fail any operational test are removed from their screener duties and must complete remedial training prior to returning to duty. Current guidance to FSDs on remedial training is that each screener must review all pertinent sections of the standard operating procedures (SOP) and Basic Screener Training modules or the appropriate recurrent training modules.

---

[1] The Federal Security Director (FSD) is the senior TSA security official responsible for aviation security operations at one or more airports. TSA currently has 159 FSDs responsible for over 400 commercial airports. Our FSDs come from many security related occupations including aviation or other transportation security disciplines, the armed forces, as well as federal, state, and local law enforcement officials.

Maintaining a high level of screener proficiency requires constant diligence. Two important elements of TSA's plan for screener improvement are recurrent screener training and supervisory training. Recurrent training is needed to maintain and enhance the skills of screeners, particularly in the areas of x-ray image interpretation, the search of persons, and the inspection of property. Supervisory training will enhance leadership skills in our workforce and provide the advanced technical skills needed to adequately supervise the screening process and resolve alarms.

Our recurrent training program is under development, though two modules have already been delivered to the field. In the meantime, FSDs have been encouraged to use the training modules of the Basic Screener Course to address specific recurrent training needs. Many have done so, and others have developed their own supplementary training. Also, screeners are required to undergo weekly x-ray image interpretation training using state-of-the-art computer-based training. FSDs at airports have received the first of a series of screener performance improvement videos and more than 350 courses will be available via our new Online Learning Center or through access to compact discs. We are also certifying over 800 screeners and training coordinators to teach various topics at each airport.

Recently, approximately 500 of TSA's 3600 screener supervisors completed the U.S. Department of Agriculture (USDA) Graduate School Introduction to Supervision course. This course is being modified to make it airport screening specific and will be introduced nationally this December. Further tailoring of the course has begun so that its content better meets the needs of screening supervisors, and we expect this enhanced course will be offered in March 2004. Our plan calls for all supervisors to complete supervisor training classes in six months.

All screeners must meet annual recertification standards, which require passenger screeners to pass an Image Certification Test, SOP Job Knowledge Test, and Practical Skills Demonstration, and require checked baggage screeners to pass an SOP Job Knowledge Test and Practical Skills Demonstration. In addition to passing these tests, developed at the national level, FSDs will be responsible for ensuring that all screeners have a satisfactory record of performance in accordance with their individual performance management plan. Recertification for 2003-2004 began on October 1, 2003, and will run through March 2004. Screeners that fail to pass any of the recertification components will be terminated. As part of our recent rightsizing effort, approximately 28,000 screeners completed portions of the proficiency testing. We will consider successful completion of those tests to be a part of the annual recertification.

3. Increased Frequency of Internal Affairs Covert Testing. To help improve screener performance, TSA will increase the number of unannounced, covert tests at airports across the Nation to assess system and airport-specific screening performance. OIAPR's testing plan is designed to test all of the airports during a three year period with Category X airports tested annually, Category I and II airports tested biannually, and contract

screener pilot[2] airports tested semiannually. Additional testing may be performed by each FSD.

Timely feedback on the results of these tests is provided to screeners, FSDs, and other TSA officials to drive change and improvement through modification of our SOPs, remedial training, and/or improving technology, as appropriate. The covert tests serve as one of many indicators of screener performance. They must be viewed in the context of a larger performance measurement system that includes individual screener TIP data, annual screener certification, supervisory oversight, the adequacy of our SOPs, and the reliability of equipment and technology.

4. Human Performance Improvements. A key element to improving screener performance is to understand the impact of screening tools, technologies, operating procedures, and environmental factors on screeners' abilities to perform their tasks. We are conducting studies to determine the causes and solutions for individual screener errors, team errors, communications breakdowns, and possible technology and procedural bottlenecks. These studies will help establish baselines, enabling us to evaluate and measure the potential impact of new technologies and procedures before they are implemented.

5. New Screening Technology. Technology is an absolute necessity in detecting threats. TSA has a robust research and development program and works closely with the DHS Science and Technology (S&T) Directorate to develop and deploy technology that will help make our operations more effective, more efficient, less time consuming, and less costly. TSA has a state-of-the-art research laboratory, the Transportation Security Laboratory, located in Atlantic City, New Jersey. To help our screeners better identify explosives and weapons that an individual may attempt to carry into the cabin of an aircraft, we are testing two explosives trace detection portals that analyze the air for explosives as passengers pass through them. TSA has also established a new performance standard for walk through metal detectors (WTMD) and replaced every WTMD at all U.S. commercial airports with the latest technology. We are developing a document scanner that will detect traces of explosives on a boarding pass type document handled by a passenger. We are also evaluating "body scan" technologies, such as backscatter x-ray, millimeter wave energy analysis, and terahertz wave technology, but will not consider deployment on any of these technologies until sufficient safeguards are put in place to ensure the protection of passenger privacy.

We are continuing to work on identifying the next generation of explosives detection equipment for use in screening carry-on and checked baggage. We are working with the vendors of the currently deployed technology to develop enhancements to existing EDS platforms to improve alarm rates, throughput, and reliability. We are simultaneously working with new vendors to develop technologies that will enable us to detect explosives in smaller amounts than are currently established in our certification standard

[2] TSA is operating a pilot program at five airports using private screeners that must meet all TSA eligibility, training, and performance requirements and receive pay and other benefits equal to those of TSA screeners

and will occupy a smaller footprint at already overcrowded airports. TSA is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat.

6. Complete 100 Percent Threat Image Projection (TIP) System Deployment. Another major initiative to improve screener performance is the implementation of an enhanced version of the TIP system. TIP superimposes threat images on x-ray screens during actual operations and records whether or not screeners identify the threat object. This tool is excellent for evaluating the skills of each individual screener so that we can focus directly on areas needing skill improvement. By regularly exposing screeners to a variety of threat object images, TIP provides continuous on-the-job training and immediate feedback and remediation. TIP allows supervisors to closely monitor screener performance and improvement.

TSA is expediting the replacement of approximately 1,800 conventional x-ray machines with TIP-ready x-ray machines (TRXs). We now have over 1,300 new TRXs in place.

Our TIP system is an improvement over the predecessor FAA system in several respects. The Federal Aviation Administration (FAA) created a library of only a few hundred images, which when shared with screeners, eliminated any real test value. In contrast, we are deploying a more comprehensive library of 2,400 images. We expect the new TSA TIP image library to be deployed on all TRX machines that are in place by the end of this calendar year. Through the combination of increased deployment of TRX machines and deployment of the expanded TIP image library, we will be able to collect and analyze significant amounts of performance data that had not been previously available to us. As we continue to deploy the expanded TIP library on all TRXs, we will primarily rely on using the limited library as an on-going training tool. Once TSA has the expanded TIP library on all TRXs in place, we will collect and analyze the data. The analysis will allow us to establish our first, national baseline view of screener performance, as measured by TIP, using the fully expanded TIP library of 2,400 images. This baseline view will help us better understand our strengths and weaknesses, allowing us to develop and implement appropriate skill enhancement strategies.

7. Expedite IT Connectivity to Checkpoints and Training Computers. TSA is taking action to deliver connectivity to all TSA locations within airports across the country. This will provide the capability for continuous training, including real-time training on current threats; greater capacity for monitoring TIP performance; connectivity with checked baggage areas; and a foundation for planned implementations of additional administrative, surveillance, CAPPS II, and other security enhancements. Unfortunately, the screening system that TSA inherited did not include this key element, and it has been both costly and time consuming to get where we would like to be in this area.

8. Update Aviation Operations Policy, Procedures, and Practice. We are updating our policies, procedures, and practices based on the lessons we have learned over the first year of Federal screening. Aviation travel is dynamic, demanding an agile system of

reevaluation and response. This process will be ongoing based on field experience and new intelligence.

In addition, TSA, working with the DHS S&T Directorate, will begin a comprehensive review of the civil aviation security system now that two years have passed since the enactment of the Aviation and Transportation Security Act and over twelve years have passed since the enactment of the Aviation Security Improvement Act of 1990. This is part of our constant evaluation of the security measures we have put into place, and now we have time to consider other approaches to aviation security that may be available to us.

9. Improve Workforce Management Scheduling and Staffing. To manage our workforce most effectively, we are exploring new methods and tools to allocate our workforce resources. We are paying close attention to human performance issues, technology limitations, and scheduling needs. There are tradeoffs that must be carefully considered such as the potential for a decreased performance level during long shifts. Recognizing that most airports have peaks and valleys in daily passenger activity, particularly at smaller airports, we are converting the workforce to a mix of full- and part-time screeners tailored to each airport. This approach will provide a better match of screener staffing with actual passenger levels at any given time.

Although ATSA mandated the federalization of airport security screening, it held open the possibility that airports could return to contract screening, provided the high standards required of the Federal screening system could be met. TSA is currently operating a pilot program at five airports using private screeners that, by law, must meet TSA eligibility, training, and performance requirements and receive pay and other benefits not less than those of TSA screeners. Beginning on November 19, 2004, any airport operator may apply to have screening performed by a contract screening company under contract with TSA. TSA is assessing if and how it will expand contract screening and to help us make these decisions recently awarded a contract to perform a rigorous assessment of the screening pilots. We will provide a program strategy and plan well before November 19, 2004.

In addition to improving screening at airports, TSA is working hard to improve airport perimeter surveillance and protection. TSA and the FAA have helped fund many local airport projects to improve perimeter security, such as construction of perimeter access roads, installation of access control systems, electronic surveillance and intrusion detection systems, and security fencing. We are currently focusing on four key areas and related technology projects: (1) security of access control through intended entry points; (2) security surveillance of perimeter areas; (3) improved security response capability to intrusions and security breaches through automated decision aids; and (4) oversight of industry compliance with current security requirements. TSA has collected and catalogued information on more than 300 applicable security technologies that include: biometrics, detection and prevention devices, surveillance technologies, and proximity sensors. Testing and evaluation of these and other technologies will be performed by

TSA in partnership with airport operators who have volunteered to be participants in a pilot program.

To ensure and improve its organizational effectiveness across the board, TSA has established performance planning and reporting mechanisms and continues to use these systems to collect data to monitor our progress toward achieving its goals. By managing this data in a central repository, TSA can assess equipment and personnel needs and status and make tactical decisions based on performance. Our Performance Measurement Information System (PMIS) was developed to capture basic performance measures at the airports on a daily basis and is continually being updated to reflect new requirements. TSA can proactively capture and analyze data on its security operations and adjust operations to achieve desired performance goals. Random and routine inspections, plus program evaluations, are also conducted to supplement the information captured by PMIS.

TSA is working to finalize and implement a set of new screener and screening system performance measures. TSA has already created the Customer Satisfaction Index for Aviation Security Operations (CSI-A), a succinct measure of our success in providing world-class customer service. The CSI-A is based on four inputs: passenger surveys at airports, a national poll, complaints and compliments made at airports about security, and complaints and compliments received at our TSA contact center. Data from each of these four inputs are scored and aggregated to form the CSI-A.

TSA is well on its way toward implementation of another important tool in its system-of systems of security, the second-generation Computer Assisted Passenger Prescreening System (CAPPS II). We appreciate the opportunity that we had to testify on the CAPPS II program before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census this past May. CAPPS II will greatly enhance our ability to keep terrorists off of commercial airlines without disturbing the efficient flow of passengers or compromising their privacy. It will also help us focus our screening resources where they will be used most effectively. CAPPS II is intended to identify terrorists and other high-risk individuals before they board commercial airplanes. CAPPS II will conduct a risk assessment of each passenger using national security information and information provided by passengers during the reservation process—including name, date of birth, home address and home phone number—and provide a "risk score" to TSA. The "risk score" includes an "authentication score" provided by running passenger name record (PNR) data against commercial databases to indicate a confidence level in each passenger's identity. CAPPS II will be a threat-based system under the direct control of the Federal government and will represent a major improvement over the decentralized, airline-controlled system currently in place.

In developing CAPPS II, TSA is very mindful of the rights, liberties, and freedoms that define our Nation and differentiate our society from those who seek to harm us. CAPPS II is being designed and will be built with the explicit requirement that privacy protection not become a cost of increased aviation security. CAPPS II is undergoing a rigorous course of testing and will not be implemented until it has successfully passed

this test phase. As part of its ongoing dialogue with the public on CAPPS II and related issues, DHS issued a revised Interim Final Privacy Notice, which provides information regarding CAPPS II, including the type of data that the system will review, and how the data will be used. The Notice requested public comment, and the closing date for submission of comments was September 30, 2003. We are now in the process of reviewing the many comments we received. TSA is also cooperating fully with the U.S. General Accounting Office (GAO) so that GAO can issue the report called for in the Department of Homeland Security Appropriations Act, 2004, by February 15, 2004.

Cargo security on passenger aircraft is a concern for all of us engaged in transportation security. This week, Secretary Ridge announced important new steps in our efforts to have the best possible protection for air cargo. TSA has issued security directives to require random inspection of air cargo and to require foreign all-cargo air carriers to comply with the same cargo security procedures that domestic air carriers must follow. These actions are building blocks in a comprehensive Air Cargo Strategic Plan that uses a threat-based, risk managed approach. The Plan is based on recommendations of working groups of TSA's Aviation Security Advisory Committee, as well as recommendations from the GAO and the Department of Transportation's Office of Inspector General.

With the holiday travel season upon us, TSA will work hard to minimize the long lines that we see normally this time of year. Travelers are another critical partner in aviation security, and they can do their part by conscientiously avoiding carrying prohibited items and following tips to help security lines flow more smoothly. As we did last year at this time, we are carrying out a major public outreach effort for air travelers.

TSA appreciates this first opportunity to appear before the full Government Reform Committee to discuss its broad strategy for aviation security and to explain its strategy for improving screener performance. Since the tragic events of September 11, 2001, we have worked very hard and have come a long way in answering the Nation's call to improve the civil aviation security system. We better understand the threats to security and have dramatically improved our capability to share information on threats. We have built a highly skilled and professional screening force and greatly enhanced security technology at airports. We know that we must be alert for new threats and must continually assess and revise our systems to meet these threats. We have all learned a great deal very quickly, and we are using every tool at our disposal to drive toward excellence.

I will be happy to answer any questions you may have.